



FortiADC - 2FA Script Deployment Guide

Version 5.4.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 20, 2020

FortiADC 5.4.1 2FA Script Deployment Guide

01-540-600000-20200220

TABLE OF CONTENTS

Change Log	4
Introduction	5
Deploying FortiADC-VM on 2FA Script	6
Step 1: Create a tokengroup	6
Step 2: Configure the pre-defined script	6
Step 3: Link these scripts to the VS	7
Step 4: Link the tokengroup to the VS.	7
Step 5: Access the my2f page from client.	7
Step 6: Try to turn on the 2FA feature by user account.	8
Step 7: Verify the 2FA feature is enabled under AUTH_ROOT_PATH folder	9

Change Log

Date	Change Description
2018-09-24	Initial release.
2018-10-18	Cannot generate tagged PDF (MadCap bug); target updated.

Introduction

FortiADC 2FA provides stronger security for authentication when the client uses a FortiADC local account to login to the Virtual Server (VS). In addition to a username and password, you will need the correct token (given by phone) to confirm your login into the VS.

Before you begin, you must do the following:

- Configure "User Authentication Settings" on the Virtual Server
- Download the FortiToken or Google Authenticator app on your mobile phone.
- Ensure that the time on the FortiADC and the mobile phone are the same.

Deploying FortiADC-VM on 2FA Script

Step 1: Create a tokengroup

FortiADC-VM # config system tokengroup

FortiADC-VM (tokengroup) # edit 1

FortiADC-VM (1) # end

FortiADC-VM #

Step 2: Configure the pre-defined script

1. TWO_STEP_VERIFICATION
2. TWO_STEP_VERIFICATION_2_SAME

The keys of the parameter:

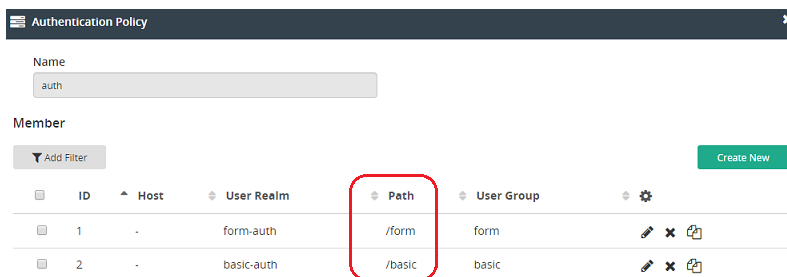
- AUTH_ROOT_PATH—The authentication folder under "User Authentication" settings. One is for the form method and the other for the basic.
- TG_NAME —Use the tokengroup entry from Step 1.

```

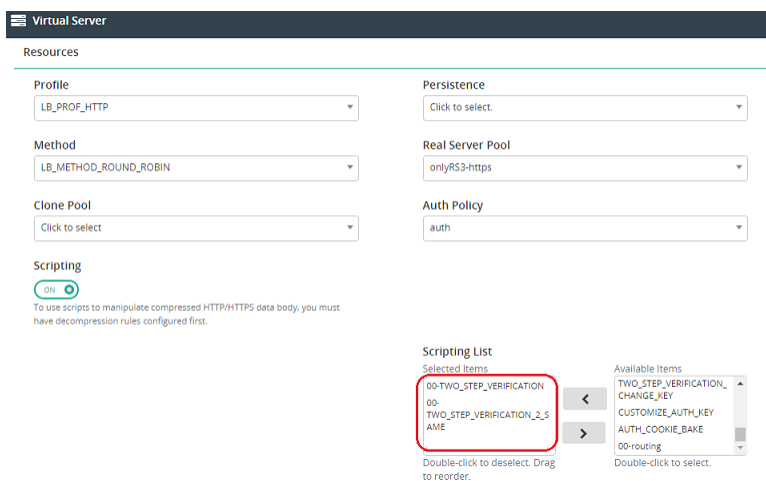
81 COOKIE_TIMEOUT_GRACE = 60;
82 AUTH_ROOT_PATH = "/form" --this shall match the path in the authentication policy
83 SIGNOUT_PATH = AUTH_ROOT_PATH."/signout2f"; --needs be lower case
84 ENABLE_PATH = AUTH_ROOT_PATH."/enable2f"; --needs be lower case
85 DISABLE_PATH = AUTH_ROOT_PATH."/disable2f"; --needs be lower case
86 ACCOUNT_PATH = AUTH_ROOT_PATH."/my2f"; --needs be lower case
87 INDEX_PATH = "50x.html";--this is relative to the AUTH_ROOT_PATH
88 IMAGE_PATH = "image/Penguins.jpg";--you need put this image on the backend real server relative to the AUTH_ROOT_PATH
89 HA_FLAG = false; --or false, set to true if you have HA setup
90 SYNC_AMONG_VS_SHARING_TOKENGROUP_FLAG = false; --or false, set to true if want to sync up the token group change among
91 map2f={};
92 when2f={};
93 tmpmap2f={};
94 status2f={};
95 INIT_TOKEN_STATUS2F = 1;
96 VIEW_2F_STATUS2F = 2;
97 ENABLE_TOKEN_STATUS2F = 3;
98 DISABLE_TOKEN_STATUS2F = 4;
99 env={};
100 TG_NAME = "1";--this is the token group selected in the virtual server
101 COOKIE_KEY = key_gen("cookiepass", "salt", 32, 32);--you need change the password phrase, don't share it with others
  
```

```

1 --This is for the second authentication group using the same token group.
2
3 when RULE_INIT priority 501 {
4   AUTH_ROOT_PATH2 = "/basic" --this shall match the path in the authentication policy
5   SIGNOUT_PATH2 = AUTH_ROOT_PATH2."/signout2f"; --needs be lower case
6   ENABLE_PATH2 = AUTH_ROOT_PATH2."/enable2f"; --needs be lower case
7   DISABLE_PATH2 = AUTH_ROOT_PATH2."/disable2f"; --needs be lower case
8   ACCOUNT_PATH2 = AUTH_ROOT_PATH2."/my2f"; --needs be lower case
  
```



Step 3: Link these scripts to the VS



Step 4: Link the tokengroup to the VS.

```
FortiADC-VM # config load-balance virtual-server
FortiADC-VM (virtual-server) # edit http-60
FortiADC-VM (http-60) # set token-group-list 1
FortiADC-VM (http-60) # end
FortiADC-VM #
```

Step 5: Access the my2f page from client.

1. Access the VS page under AUTH_ROOT_PATH/my2f and input the correct user/passwd.
2. Input the password again.
3. You will see the 2FA summary page.

Web Authentication

UserName: form

Password: [masked]

Login

form, Let's make sure it's really you! Enter password:

Powered by FADC

Entering 2-Step Verification

Password: [masked]

Submit

2-Step Verification

User Name: form

Status: OFF

Powered by FADC

2-Step Verification Summary Turn-on or Change 2-Step Verification

Turn-off 2-Step Verification Sign-Out 2-Step Verification Index Page

Step 6: Try to turn on the 2FA feature by user account.

1. Click the **Turn-on or Change 2-Step Verification** to turn on the feature.
2. Will require to scan a QR code to input the information on the APP.
3. Input the token for confirmation.
4. Check if the status is ON on the my2f page.

2-Step Verification

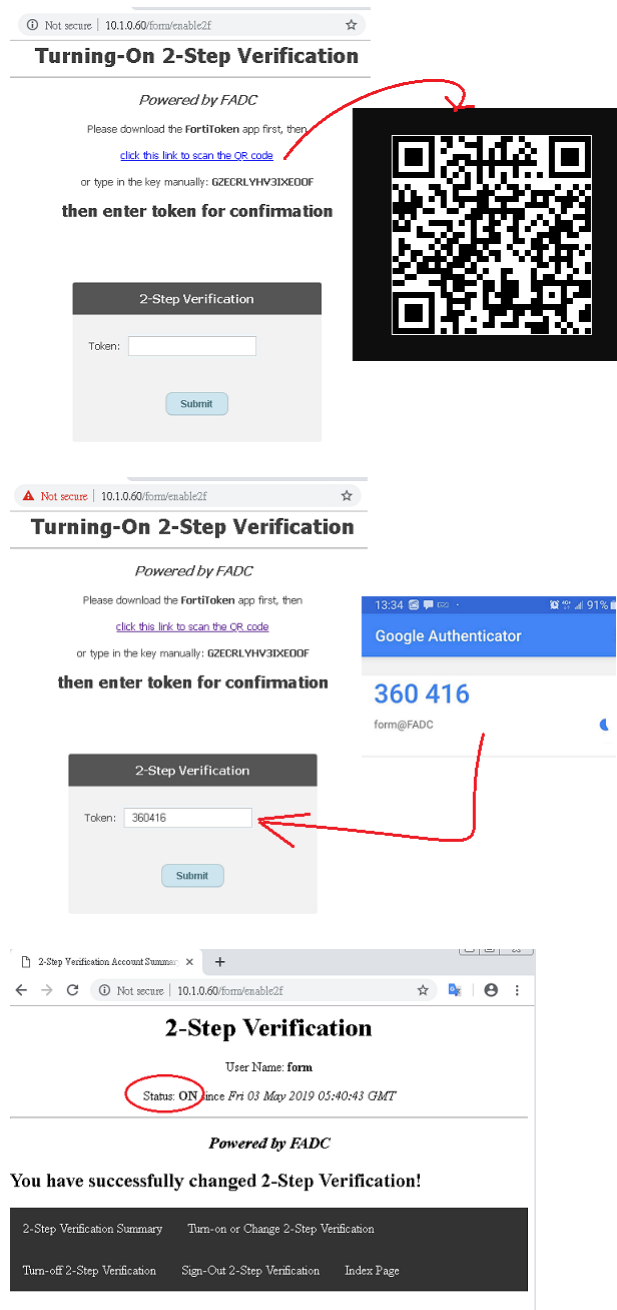
User Name: form

Status: OFF

Powered by FADC

2-Step Verification Summary **Turn-on or Change 2-Step Verification**

Turn-off 2-Step Verification Sign-Out 2-Step Verification Index Page



Step 7: Verify the 2FA feature is enabled under AUTH_ROOT_PATH folder

1. Access the page <http://VS/form/index.htm>
2. Input the username and password.
3. Input the token for the 2FA verification.
4. You will see the index.htm content.

▲ Not secure | 10.1.0.60/form/index.htm

Web Authentication

UserName:

Password:

2-Step Verification

2-Step Login for Extra Security

Powered by FADC

2-Step Verification

Token:

10.1.0.60/form/index.htm

Not secure | 10.1.0.60/form/index.htm

Test FORM-HTML Test



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.